REMARKS

The Office Action mailed May 11, 2007 considered claims 12, 14-22, 34, and 36-60. Claims 45-51, 53, 58 and 60 were rejected under 35 U.S.C. 102(b) as being anticipated by Check point (NPL "Check Point FireWall-1 User Guide", books "Architecture and Administration" – AA, and "Virtual Private Networking with Check Point FireWall-1" – VP) hereinafter *Checkpoint*. Claims 12, 14-22, 34, 36-44, and 54-57 were rejected under 35 U.S.C. 103(a) as being unpatentable over *Checkpoint*, and further in view of Boroditsky et al. (US 6,332,192) hereinafter *Boroditsky*. Claims 52 and 59 were rejected under 35 U.S.C. 103(a) as being unpatentable over *Checkpoint*.[1]

By this amendment, claims 12, 34, 36, 38, 45, 48 and 54-58 have been amended.[2] Claims 12, 14-22, 34, and 36-58 are pending, of which claims 12, 34, 45, and 58 are the only independent claims at issue.

Embodiments of present invention are directed authenticating computer systems that are connected to and/or communicating with virtual private networks. Claim 12, for example, defines receiving an assertion from the client that the client has credentials appropriate for accessing the private network resource. Next, claim 12 defines initiating a plurality of authentication transactions between the client and the firewall, the plurality of authentication transactions designed to impose commensurable processing burdens on the client requesting access to the private network resource and the firewall operating as a gateway for the private network to mitigate the potential of a client performing a denial of service attack against the private network, wherein the client initially is unaware that the firewall operates as a gateway for the private network, and wherein successful completion of each authentication transaction incrementally increases a level of trust between the client and the firewall.

Next, claim 12 defines, for each of the plurality of authentication transactions between the client and the firewall, using a zero-knowledge proof to challenge the client for credentials, the zero-knowledge proof including sending a challenge to the client, the correct answer to the challenge obtainable from the asserted credentials without having to arrange the credentials

[1] Although the prior art status of the cited art is not being challenged at this time, Applicant reserves the right to challenge the prior art status of the cited art at any appropriate time, should it arise. Accordingly, any arguments and amendments made herein should not be construed as acquiescing to any prior art status of the cited art.

[2] Support for the amendments to the claims are found throughout the specification and previously presented claims, including but not limited to paragraphs [0036]-[0038] and Figures 3 & 4.

according to a specified layout and without even having to divulge the asserted credentials such that if the client actually possesses the asserted credentials the client can generate the correct answer, receiving a response from the client including an answer to the challenge, the answer including at least some measure of proof that the client has credentials and that the client's credentials are correct, and verifying whether or not the answer included in the response the correct answer to the challenge. Lastly, claim 12 defines when an acceptable level of probability that the client actually possesses the asserted credentials is reached based on a plurality of correct answers, the firewall granting the client access to the private network resource through the firewall for processing of the asserted credentials.

Claim 34 is a computer-readable media claim corresponding to claim 12. Claim 45 is a method claim similar to claim 12, but from the perspective of the firewall. Claim 58 is a computer-readable media claim corresponding to claim 45.

Chapter 1 of the architecture and Administration (or "AA") portion of *Checkpoint* describes authentication at a firewall (page 27). Various different types of authentication including user authentication, client authentication, session authentication, and transparent authentication and their corresponding features are described (pages 28-29). Further, the different types of authentication can be implemented using various different authentication schemes (page 30).

When a request is directed to a server, a firewall can be invoked to mediate a connection to a server (page 31). The user can submit credentials to the firewall and then, if the firewall credentials are appropriate, be connected to a server for further authentication (pages 31-32 and 39-41). Alternately, a request can be sent directly to the firewall to gain access to the server (pages 42-44). Thus, the AA portion of *Checkpoint* essentially describes that gaining access to a server may require two separate logins, potentially based on two different sets of credentials, for example: 1) a login to a firewall and 2) a separate subsequent login to the server.

However, completing authenticating with either the firewall or the server includes receiving a request for server access, returning a request for credentials, receiving credentials, and processing the credentials. If the credentials are appropriate, the user is allowed to subsequently login at the server (authenticated at firewall), or is given server access (subsequently authenticated at server). If not the user is denied access. No other authentication related decisions are made.

Further, in *Checkpoint*, each of the firewall and server are individually responsible for their own processing. Neither can make authentication related assertions for or based on information associated with the other. Thus, while the firewall can interpose itself between a client and a server, the firewall can not assert to the client that it is trusted by the server or vice versa.

Boroditsky teaches a generalized user ID and authentication scheme. *Boroditsky* provides user access to multiple secure applications using a single login (Abs.). The login is created from a manipulation of symbols such as pictures. The manipulations are allegedly easy to remember and difficult to guess (Col. 2:37-40). For example, the authentication scheme may prompt a user to place pictures of pieces of food onto a plate in a certain layout and/or in a certain order (Col. 3:25-46). The scheme maps each picture's place on a grid and derives a code key based on the pictures' orientation (Figs. 3 & 4). The code key is then used as proof of the user's credentials and, with it, the user is able to log in to multiple secure applications. The trust and authentication process is performed once and is not iterative, nor is trust built over the course of multiple transactions.

Thus, the cited art fails to teach either singly or in combination, initiating a plurality of authentication transactions between the client and the firewall, the plurality of authentication transactions designed to impose commensurable processing burdens on the client requesting access to the private network resource and the firewall operating as a gateway for the private network to mitigate the potential of a client performing a denial of service attack against the private network, wherein the client initially is unaware that the firewall operates as a gateway for the private network, and wherein successful completion of each authentication transaction incrementally increases a level of trust between the client and the firewall, as recited in claim 12, in view of the other limitations of claim 12.

The cited art also fails to teach either singly or in combination, for each of the plurality of authentication transactions between the client and the firewall, using a zero-knowledge proof to challenge the client for credentials, the zero-knowledge proof including sending a challenge to the client, the correct answer to the challenge obtainable from the asserted credentials without having to arrange the credentials according to a specified layout and without even having to divulge the asserted credentials such that if the client actually possesses the asserted credentials the client can generate the correct answer, receiving a response from the client including an

answer to the challenge, the answer including at least some measure of proof that the client has credentials and that the client's credentials are correct, and verifying whether or not the answer included in the response the correct answer to the challenge, as recited in claim 12, in view of the other limitations of claim 12. For at least any of these reasons, claim 12 patentably defines over the art of record. For at least any of the same reasons, claims 34, 45 and 58 also patentable defines over the art of record. Since any dependent claims depend from one of the independent claims 12, 34, 45, or 58, each of the dependent claims also patentably define over the art of record at least for the same reason as their corresponding base claim.

Applicants respectfully submit that the cited art of record does not anticipate or otherwise render the amended claims unpatentable for at least the reason that the cited art does not disclose, suggest, or enable each and every element of these claims.

Claim 36 was objected to because of the following informality: "wherein the are related to at least one of a". Claim 36 has been amended to include "wherein the credentials are related to at least one of a". Accordingly, Applicants respectfully request that the objection to claim 36 be withdrawn.

Claim 38 was objected to because of the following informality: "of claim 35" (i.e. claim 38 was improperly dependant on cancelled claim 35. Claim 38 was amended to recite proper dependency on claim 34. Accordingly, Applicants respectfully request that the objection to claim 38 be withdrawn.

In view of the foregoing, Applicant respectfully submits that the other rejections to the claims are now moot and do not, therefore, need to be addressed individually at this time. It will be appreciated, however, that this should not be construed as Applicant acquiescing to any of the purported teachings or assertions made in the last action regarding the cited art or the pending application, including any official notice. Instead, Applicant reserves the right to challenge any of the purported teachings or assertions made in the last action at any appropriate time in the future, should the need arise. Furthermore, to the extent that the Examiner has relied on any Official Notice, explicitly or implicitly, Applicant specifically requests that the Examiner provide references supporting the teachings officially noticed, as well as the required motivation or suggestion to combine the relied upon notice with the other art of record.

In the event that the Examiner finds remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney at (801) 533-9800.

Dated this 11th day of July, 2007.

Respectfully submitted,

/GREGORY R. LUNT/

RICK D. NYDEGGER
Registration No. 28,651
MICHAEL B. DODD
Registration No. 46,437
GREGORY R. LUNT
Registration No. 47,354
Attorneys for Applicant
Customer No. 47973

RDN:MBD:GRL:crb
CRB0000005573V001